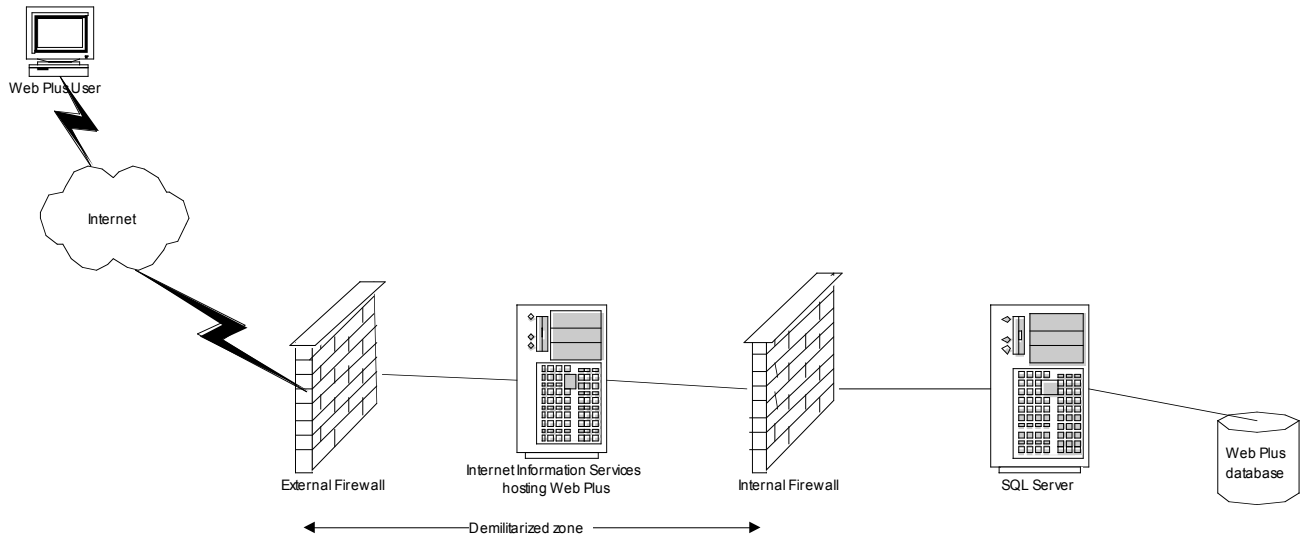
Web Plus™ Security Features and Recommendations

The Centers for Disease Control and Prevention's (CDC) National Program of Cancer Registries (NPCR) designed Web Plus as a highly secure application that can be used to transmit confidential patient data between reporting locations and a central registry safely over the public Internet. Security is achieved by a combination of software features and network infrastructure. This document outlines the security features of the application and recommendations for the operating environment to ensure a secure installation of Web Plus.

Web Plus is a form-authenticated, ASP.NET application that is hosted on Internet Information Services (IIS) running on Microsoft® Windows® 2000 or later server operating systems. In a typical setting, the web server sits in the demilitarized zone (DMZ) between the external and internal firewalls while SQL Server, where the Web Plus database is stored, resides inside the internal firewall as part of the trusted network.



The security of Web Plus depends to a large extent on the security of the client computer, the communication channel between the client and the web server, the web server, the base operating system, and the configurations of firewalls on either side of the web server. Security breaches by social engineering attacks are always a consideration—special attention is required in all parts of the system to prevent such attacks. Use of strong logon passwords for logging in to Web Plus is highly recommended, and the sharing of user accounts by users should be expressly prohibited.

Security Features of the Web Plus Application

Form-Based Authentication

Web Plus uses form-based authentication where users are required to enter their user IDs and passwords to be authenticated by the application.

Role-Based Access

Web Plus also implements a role-based access where users are granted different levels of access depending on their roles.

Currently, five roles are defined in Web Plus:

Users	Description
Facility Abstractor	Works in a local facility or doctor's office and handles patients' medical records and paperwork. When a patient is diagnosed with cancer, the facility abstractor reports the case to the state's central cancer registry.
Central Registry Abstractor/Reviewer	Reviews abstracts submitted to the central registry for completeness and accuracy and may abstract additional data items from submitted text; also abstracts new cases.
Central Registry Administrator	Sets up the local facilities with access to the Web Plus software to report their data, manages facility accounts and users at both central registry and facilities, configures display types, edit sets and system preferences, manages assignment of abstracts to central registry staff, exports data and views reports.
Local Administrator	Manages local users of a facility.
File Uploader	Uploads files of abstracts in the appropriate NAACCR format that were not abstracted using Web Plus, views EDITS error report and cleans, or works with abstractors to clean, errors on rejected files prior to re-uploading.

Other Application Security Features

Other security features of the application include:

- Facilities and offices have access only to those abstracts entered at their facility or office.
- Web Plus keeps an extensive log of user logins, data accesses, and updates for auditing purposes.
- User accounts can be locked out if invalid login attempts exceed a threshold value, configurable by the Central Administrator.
- Current user activities are visible to the Central Administrator through the Current User Activities page.
- Display types and edit set configurations are centrally controlled.
- User passwords are stored in the database using a one-way hash encryption method.
- The Web Plus configuration file can store the connection string to the SQL Server database in encrypted format.

Security Features of the Operating Infrastructure

Security on the Client Computer

The client computer should be protected from any kind of Trojan horse or spyware attacks by installing anti-virus and anti-spyware software, and ensuring that these programs are up-to-date.

Secure Communication Channel and Server Certificate

Web Plus relies on the existence of a Secure Sockets Layer (SSL) channel between the web server and client browser for the protection of data exchanged over the Internet. To set up an SSL channel, the web server needs to have a server certificate installed and the website containing the application should have SSL encryption turned on. The certificate for the server could either be created in-house, if a certificate server is available, or can be purchased from a commonly trusted third party commercial organization called a Certificate Authority (CA). A certificate of 128-bit cyber strength is the industry standard for secure communication over the Internet and is highly recommended.

Implementing Two-Factor Authentication by Using Client Certificates

The form-based authentication of Web Plus may be supplemented with a two-factor authentication scheme in which clients are authenticated based upon "what they know" and "what they have." The "what they know" part of the scheme is fulfilled by the login page of Web Plus, as users need to know their User IDs and passwords to log into the system. The "what they have" part can be implemented by configuring the Web site to require clients to have certificates to connect to it. This requires deploying Public Key Infrastructure (PKI) to clients.

Hardening of the Web Server and Operating System

Follow the guidelines from Microsoft to harden the web server and the base operating system. The IISLockdown tool available from Microsoft's download site can be used to automate several security steps to reduce the vulnerability of the Windows 2000 web server. General recommendations from Microsoft include:

- Applying the latest patches to the operating system and Internet Information Services. Use the Microsoft Baseline Security Analyzer (MSBA) to detect patches and updates that may be missing from the current installation.

- Do not install IIS as part of the operating system installation. Rather, install it later, after you have updated and patched the base operating system. Then install IIS, apply patches, and harden the IIS configuration.

- When installing IIS, do not install File Transfer Protocol (FTP Server), Microsoft FrontPage 2000 Server Extensions, Internet Service Manager (HTML), NNTP Service, Visual InterDev RAD Remote Deployment Support. However, SMTP needs to be installed to support e-mail capability of Web Plus.

- Disable unnecessary protocols: Disable NetBIOS and SMB on the Internet-facing network interface card (NIC); remove Web Distributed Authoring and Versioning (WebDAV).

- Delete or disable unused accounts: Rename the Administrator account, disable the Guest account, disable the IUSR account, create a custom anonymous Web account, enforce strong password policies, restrict remote logons, and disable null sessions. The custom anonymous account created to replace IUSR account should have the least privilege. If you run IISLockdown, add your custom user to the Web Anonymous Users group that is created. IISLockdown denies access to system utilities and the ability to write to Web content directories for the Web Anonymous Users group.

- Use strong access controls to protect sensitive files and directories. Set access at the directory level whenever possible.

- Ensure that only the .NET Framework Redistributable package is installed on the server and no SDK utilities are installed. Do not install Visual Studio.NET on production servers. Debugging tools should not be available on the web server. Ensure that access to powerful system tools and utilities, such as those contained in the \Program Files directory, is restricted. Remove all of the sample files.

- Relocate Web roots and virtual directories to a non-system partition to protect against directory traversal attacks.

Secure Connection to the Database

If SQL server authentication is used, the User ID and password are embedded in the connection string, but the connection string is stored in encrypted form (using DPAPI) in web.config. If Windows authentication is used, the user's credentials are not included in the connection string; the connection string is still encrypted, hiding the database server's IP address, port number, etc.

Windows authentication is the preferred method from a security point of view because this mode does not transmit the user's credentials over the network. For Windows authentication to work, a mirrored ASP.NET process account must be created as a local Windows account with the same name and password on the database server. ASP.NET is a least privileged account created at the time of installing the .NET Framework on the web server. By default, all ASP.NET applications run under the security context of this account. After creating the account in Windows, create a SQL Server login for the account and grant it access to Web Plus database.

It is recommended that the SQL Server listen on a port number different from the default port, 1433. This port then should be opened in the internal firewall to allow the web server to access the database.

Configuring ASP.NET for Security

Various security options can be configured in web.config and machine.config files. The settings depend on the local security requirements and administrative preferences. In most cases, leaving the settings at the default values should provide the required security.